第 37 卷第 4 期 计算机应用研究 Vol. 37 No. 4
录用定稿 Application Research of Computers Accepted Paper

抗同步化攻击的轻量级 RFID 双向认证协议 *

柳　毅[1]，陈添笑[1]，洪　洲[2]

(1. 广东工业大学 计算机学院，广州 510006; 2. 广州城市职业学院科研处，广州 510405)

摘　要：针对现有的 RFID 认证协议在安全认证过程中，由于协议的设计的缺陷，导致的协议安全性不足的问题，提出了一种利用同步化随机数以及 PUF 改进的轻量级 RFID 认证协议。首先提出了一种对 RFID 协议的去同步化攻击方法，并分析其原因；然后通过在标签和读写器两端设置一个同步化随机数，增强协议抗去同步化攻击的能力；最后，在标签中引入了 PUF，通过 PUF 的不可克隆性提高了标签密钥的抗攻击能力。分析结果表明，新协议能有效地抵抗多种攻击，在保证一定效率和开销的同时具有更高的安全性。

关键词：RFID；轻量级；物理不可克隆函数；双向认证；CRC

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.09.0756

Lightweight RFID two-way authentication protocol with anti-synchronization attack

Liu Yi[1], Chen Tianxiao[1], Hong Zhou[2]

(1. *School of Computer Science & Technology*, *Guangdong University of Technology*, *Guangzhou* 510006, *China*; 2. *Office of Academic Research*, *Guangzhou City Polytechnic*, *Guangzhou* 510405, *China*)

Abstract: In view of the existing RFID authentication protocol is insufficient in the security authentication process due to the flaws in the design of the protocol, this paper presented an improved lightweight RFID authentication protocol using synchronized random number and PUF. It first proposed a desynchronizing attack method on RFID protocols, and analyzed the reason.Then it enhanced the protocol's ability to resist desynchronization attacks by setting a synchronized random number at both ends of the tag and reader.Finally, it introduced the PUF in the tag, used the PUF's non-clonality to improve the tag's anti-attack capability. The analysis results show that the new protocol can effectively resist multiple attacks, and it has higher security while ensuring certain efficiency and overhead.

Key words: RFID; lightweight; puf; mutual-authentication; CRC

0　引言

射频识别（radio frequency identification，RFID），又称无线射频识别，是一种非接触式识别技术，可通过无线电讯号识别特定目标并读写相关数据而无须与目标物体进行物理接触。RFID 已被广泛应用于许多领域，如物流、军事、交通等。

RFID 通常由三部分组成：标签、读写器和后端数据库。后端数据库和读写器之间的通信信道一般被认为是安全可靠的[1]。读写器和标签之间的信道由于采用的是无线连接，缺乏保护非常脆弱，容易遭到窃听和欺骗。随着 RFID 技术的发展，RFID 的安全性问题得到了越来越多的重视。为了保障 RFID 的安全，设计一个安全的 RFID 认证协议具有重要意义。

RFID 标签要求低成本，所以计算能力往往不强，传统的公钥密码算法如 RSA 等，不适用于 RFID 协议。所以如何设计安全性高的、低成本的、高效的轻量级 RFID 认证协议成为当下研究的热点之一。

保持 RFID 标签的轻量性具有重要意义。文献[2,3]将传统的密码学工具应用于 RFID 协议中，虽然具有良好的安全性，但并未考虑到标签的计算力。文献[2]提出了一种基于 hash 函数和时间戳的认证协议，该协议采用了时间戳防止攻击者的重放消息，但并未对 hash 函数进行优化，导致标签计算成本过高。文献[3]提出了一种基于 *CRC* 和伪随机数发生器的轻量级协议，在传输信息过程中先用 *CRC* 的单向性进行加密，然后第一条 message 的高位与令一条 message 的低位交叉组合传送。但是标签采用了伪随机数发生器，由于 RFID 标签计算能力的局限性，协议效率不高。

为了降低标签成本和提高效率，在最早的一批超轻量级 RFID 认证协议中，使用了一些简单的运算函数和认证步骤，提高了效率但降低了安全性。Chien 提出的 SASI 协议认证过程中加入了 *Rot* 移位运算[4]，但是文献[5]随后指出了对 SASI 协议的 Dos 攻击和标签追踪攻击;文献[6]在 SASI 的基础上提出了 Gossamer 协议，协议结构基本相似，在后面的密钥更新过程中引入了 MixBits 运算，提高了安全性，但 Zeeshan 在文献[7]中提出了对该协议的去同步化攻击以及其他安全性分析。

Tian 等人在 2012 年提出了一个超轻量级的认证协议 RAPP[8]，不过随后 Eyad 等人在文献[9]中指出了对 RAPP 协议的一种抗同步攻击方法。随后文献[10]对 RAPP 协议进行了改进，提出了一种 PAPP 协议，用标签中的加密算法的单向性产生随机数，防止去同步化攻击。这种方法相比与一般的直接加随机数发生器来说，共用了标签中的门电路，减少了标签开销。

收稿日期：2018-09-27；**修回日期：**2018-10-23　**基金项目：**国家自然科学基金资助项目（61572144）；广州市教育系统创新学术团队资助项目（1201610027）

作者简介：柳毅（1976-），男，江苏连云港人，教授，博士，主要研究方向为网络与信息安全；陈添笑（1996-），男，湖南邵阳人，硕士研究生，主要研究方向为信息安全（438657459@qq.com）；洪洲（1979-），男，江西东乡人，教授，博士，主要研究方向为物联网机器人.

由于文献[4-6,8,10]的协议过于简单而存在的安全性问题。在文献[11]中，Zhang 等人对以上这批超轻量的认证协议的协议周期和安全强度进行了详细分析，结果发现这些协议采用的运算都比较简单，复杂度低，抗攻击能力弱。随后提出了一种基于哈希类函数 M-Hash 函数的认证协议 MH 协议，M-Hash 函数具有硬件资源需求低，抗碰撞性强等特性。在 MH 协议中 Zhang 等人还通过减少 M-Hash 的逻辑操作位，来提高协议的效率。Zhang 等人的协议实现了 RFID 协议安全性与效率的平衡，但 M-Hash 实现所需的门电路依然较多。

Yang 在文献[12]提出了一种新的轻量级认证协议，认证过程中采用了 *CRC* 和交叉位运算 *Cro*。该协议标签的计算量和通信量非常低，非常适用于轻量级 RFID 系统。但是经过分析协议并不能抵抗去同步化攻击且仅仅依靠 *CRC* 和 *Cro* 这些简单的运算更新密钥安全性不高。

为了解决文献[12]中的安全性问题，文章结合一个同步化随机数和物理不可克隆函数(PUF)在该协议的基础上进行改进，提出一种新的轻量级认证协议。旨在保持协议低成本的同时具有更高的安全性。物理不可克隆函数(PUF)是一个利用物理特征把输入值映射到应答值的函数[13]。PUF 具有不可克隆性，每给定一个输入，都会得到一个唯一且不可预测的输出。对于相同的输入，每个 PUF 的输出都不同。

1　对 Yang 的协议的分析

1.1　符号描述

ID:标签真实身份标志

TID^{old}:上一轮标签临时身份标志

TID^{new}:本轮的标签临时身份标志

K_i^{old}:标签和读写器上一轮共享密钥(i=1,2)

K_i^{new}:标签和读写器本轮的共享密钥(i=1,2)

N_i:读写器生成的随机数(i=1,2)

r_n:读写器和标签初始的同步化随机数。

A-E:读写器和标签之间的交换信息

⊕:按位异或运算

$Cro(X,Y)$:交叉位运算

CRC-16(X):循环校验函数，加密 X 的值

(G_n, G_{n+1}):PUF 初始验证对。

PUF(X):随机置换函数(通过 PUF 实现)。

1.2　Yang 的协议描述

Yang 的协议如图 1 所示，下面给出对于 Yang 的协议的一种去同步化攻击：

a）在第 n 次认证的时候，阻塞认证协议第⑤步，使得读写器更新了密钥以及标签的临时身份 *TID* 而标签没有跟新。此时读写器拥有的信息是(TID^{n+1}_{new}，TID^{n}_{old}，$K^{n+1}_{i new}$ (i=1,2,3),$K^{n}_{i old}$ (i=1,2,3)),标签拥有的信息为(TID^{n}_{old}, $K^{n}_{i old}$(i=1,2,3))。并窃听到他们第 n 次认证的通信消息 $Hello^n$、$A||B^n$、C^n、$D||E^n$。此时标签和读写器依然能相互认证。

b)在第 n+1 次认证的时候，再次阻塞认证协议第⑤步。此时读写器拥有的信息是(TID^{n+2}_{new}，TID^{n}_{old}，$K^{n+2}_{i new}$ (i=1,2,3),$K^{n}_{i old}$ (i=1,2,3)),标签拥有的信息为(TID^{n}_{old}, $K^{n}_{i old}$(i=1,2,3))。

c)重放第一步中听到的消息，首先读写器向标签发送 $Hello^n$，标签返回他的 TID^{n}_{old}，再按照步骤发送 $A||B^n$和 $D||E^n$给标签。重放过后，标签中的信息为(TID^{n+1}_{new}, $K^{n+1}_{i new}$(i=1,2,3))。而此时读写器中的信息为(TID^{n+2}_{new}，TID^{n}_{old}，$K^{n+2}_{i new}$ (i=1,2,3),$K^{n}_{i old}$ (i=1,2,3))，则标签和读写器之间不能进行验证。

攻击者通过上述步骤能使被攻击过后的标签不能被读写器认证，从而实现了对协议的去同步化攻击。

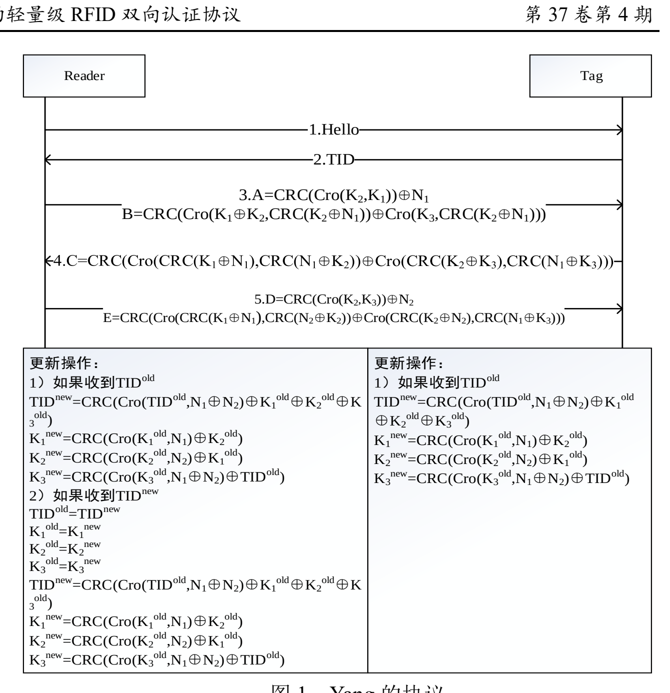


图 1　Yang 的协议

Fig. 1　Yang's protocol

Yang 的协议之所以会存在该问题最主要的原因是在标签没有更新的一定时间段内，对于每一个 *A*、*B* 消息的响应消息都是一样的。这种情况也导致了可以对其进行跟踪攻击。攻击者可以在每次验证时阻断标签密钥更新，随后通过发送之前一样的消息 *A*、*B* 得到相同的回应，从而实现跟踪攻击。

一般对于这种安全问题的改进方法通常是增加一个随机数发生器，文献[14]的协议也存在类似去同步化问题，文献[15]对其用随机数发生器进行了改进，虽然利用加密算法的一部分产生随机数，但仍有一定的计算量。本节采用同步化随机数和物理不可克隆函数(PUF)在 Yang 的协议的基础上进行改进，提出了一种新的轻量级协议。

2　新的协议

协议的符号说明与 1.1 节相同。新协议如图 2 所示。

协议初始阶段读写器中持有相应 PUF 事先生成好的验证对(G_n, G_{n+1}),密钥 K_1,K_2,同步随机数 r_n。标签中持有{ID,TID,K_1,K_2,r_n}。

协议过程详细描述如下：

①*Hello*：读写器向标签发送“*Hello*”信号发起验证，协议认证过程开始。

②*TID*：标签收请求后，将自身的临时身份 *TID* 发给读写器，读写器将此 *TID* 传到后台的数据库中进行查找，若能够找到对应的 *TID*，则后台数据库将与之相匹配的密钥 K_i 发送给读写器，标签和读写器开启双向认证阶段。若该 *TID* 在数据库中不存在，则认证失败，需重新开始认证。

③*A* 和 *B*:双向认证阶段中，读写器产生两个随机数 N_1,N_2，计算 *A* 和 *B* 发送给标签，请求标签通过 PUF 计算进行验证。发送完成后读写器计算 r_{n+1}=CRC(r_n⊕N_1)。标签通过密钥 K_1,K_2，提取出 *A* 中的 G_n 用于随后的 PUF 计算，然后用 K_1,K_2, G_n 计算得到 *B* 中的随机数 N_1。

④*R* 和 *C*:标签利用 PUF()函数和读写器发过来的 G_n 和计算 PUF(G_n)得到 G_{n+1}，再计算 G_{n+2}=PUF(G_{n+1})和 r_{n+1}=CRC(r_n⊕N_1)，利用密钥 K_1,K_2, N_1, r_{n+1}, G_{n+1} 和 G_{n+2} 计算 *R* 和 *C* 发送给读写器。同样，读写器先从 *R* 中得到标签发送过来的 G_{n+1}，并与自己的 G_{n+1} 进行比较，若相等，则读写器对标签认证成功。若不相等，认证失败。

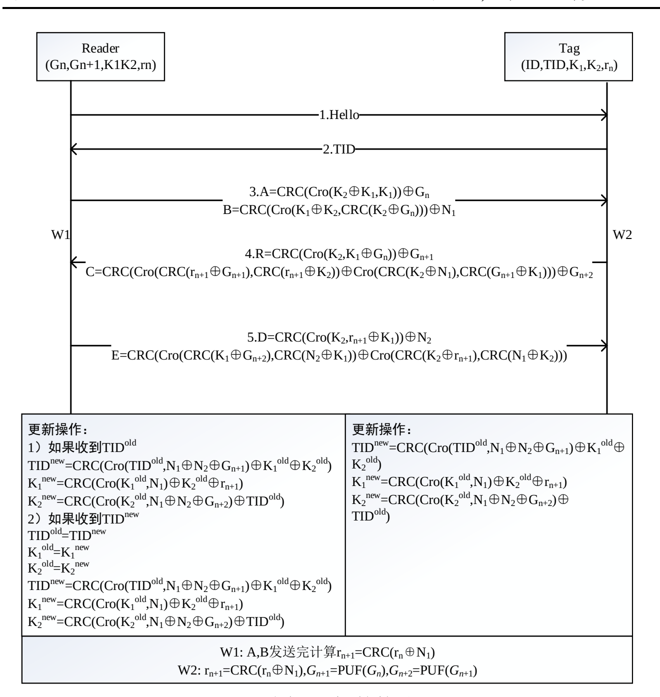


图 2　新的协议

Fig. 2　The new protocol

认证成功后再用 K_1,K_2，N_1，r_{n+1}，G_{n+1} 计算得到 C 中的 G_{n+2}，(G_{n+1} ,G_{n+2})作为下一次读写器认证和标签的 PUF 验证对，随后读写器进行密钥更新。

⑤D 和 E:读写器用之前生成的随机数 N_2 计算 D 和 E 并发送给标签,标签提取 D 中的 N_2 并计算 E'与 E 进行比较，若相等，则说明读写器得到了 G_{n+2} 并拥有正确的 r_{n+1}，标签对读写器认证成功。用随机数 N_1,N_2 和 r_{n+1},G_{n+1} ,G_{n+2} 更新自己的密钥，协议结束。若不相等，则认证失败且不更新密钥。

新协议通过在标签和读写器中同步了一个随机数使得协议具有能力抵抗攻击者的去同步化攻击，且该随机数不需要标签发送，减少了通信量。

PUF 的使用增强了协议的安全性，在协议某轮中即使攻击者通过某种方式得到（G_n，G_{n+1}），攻击者无法逆向推导出之前使用的认证对，以及推出之后使用的认证对。使标签认证相比于之前的 *CRC* 更新的密钥更安全。

3　协议的安全性分析

本节将对改进后的协议进行安全性分析，具体从假冒攻击、信息泄露攻击、跟踪攻击、克隆攻击、重放攻击、去同步化攻击、后向安全性以及双向认证八个方面说明改进后的协议的安全性。说明了新的协议能抵抗之前提到的去同步化攻击的原因。

1）假冒攻击

假冒攻击是指攻击者冒充标签或读写器进行认证，试图得到一些有用的认证信息的一种攻击。在改进后的协议中，无论协议的那一部分被修改,标签和读写器都是可以发现的。因为 K_i,N_1,N_2, r_{n+1} 以及 PUF 产生的认证对都是动态变化的，且协议中每一步读写器和标签都能进行认证，攻击者没有相应的 K_i 和认证对无法假冒标签和读写器进行完整的认证。攻击者通过假冒攻击最多只可能得到 *TID*，除此之外得不到任何有价值的信息。而 *TID* 只是一个临时的身份标志，并且每轮认证成功后都会改变，没有实际意义，故该协议能够抵抗假冒攻击。

2）信息泄露攻击

信息泄露攻击是指攻击者对来自读写器的消息进行特定的修改，然后发送给标签，从标签的响应中推出协议的相关信息[13]。由于本协议中每个步骤都是加密的或随机的，所用的 N_1,N_2 和 r_{n+1},G_{n+1} ,G_{n+2} 也都是经过 *CRC* 和 *Cro* 加密传输，且在读写器和标签每一次收到消息时，都会对其进行验证，若验证失败，协议将被终止。所以当攻击者试图修改协议中的任何一个信息时，都会被认证发现，协议将被终止，故该协议能够抵抗信息泄露攻击。

3）跟踪攻击

协议的整个过程中都是使用标签临时的 *TID* 来作为标签的身份标志，协议的整个过程都没有标签真实的 *ID* 出现，所以攻击者无法通过截获的协议内容得到标签的真实身份 *ID*，从而无法对 ID 进行跟踪。若攻击者想对某个截获的标签 *TID* 进行跟踪，由于 *TID* 每轮协议完成后都会由随机数 N_1,N_2 和 G_{n+1} 进行更新，所以由 *TID* 对标签的跟踪攻击也无法实现。故该协议能抵抗跟踪攻击。

4）克隆攻击

对于克隆攻击，本协议采用了物理不可克隆函数 PUF 产生的验证对作为标签每轮认证读写器的方法。由于 PUF 的不可克隆特性，攻击者没办法伪造出和该标签中 PUF 一模一样的 PUF，从而无法克隆出一个含有合法的 PUF 的标签。故本协议能够抵抗克隆攻击。

5）重放攻击

每当一轮协议运行成功结束时，读写器和标签中的密钥 K_i，同步化随机数 r_n 以及 *TID* 等都会改变。假设攻击者假装读写器对标签进行重放攻击，首先重放第一步的 *Hello*，标签返回更新后的 *TID*，在重放第三步的消息 *A,B*,然而经过了上轮的更新后，*A,B* 中的密钥 K_i 并不能对应更新后的 *TID*。所以即使攻击者截取上一轮的认证信息进行重放，也通过不了认证。故该协议能够抵抗重放攻击。

6）去同步化攻击

改进后的协议能抵抗之前提到的对原协议的去同步化攻击。原理是通过在标签和读写器中加入了一个同步化随机数 r_n。读写器每次第三步请求标签时，读写器都会计算新的 r_{n+1}=CRC($r_n\oplus N_1$)，当标签接收到读写器发来的请求时，也会计算一个同样的 r_{n+1}。从而保障了第四步的信息 *C* 每轮都不一样，因此新协议具有抗该种去同步化攻击的能力。

对于之前的去同步化攻击在新协议的情况下：

a）同样的在第 n 次认证的时候，阻塞认证协议第⑤步，使得读写器更新了密钥以及标签的临时身份 *TID* 而标签没有跟新。此时读写器拥有的信息是(TID^{n+1}_{new}，TID^{n}_{old}，K^{n+1}_{inew}(i=1,2)，K^{n}_{iold}(i=1,2)，G_{n+1}，G_{n+2}，r_{n+1}，*ID*)，标签拥有的信息为(TID^{n}_{old}，K^{n}_{iold}(i=1,2)，*ID*，r_{n+1})。并窃听到他们第 n 次认证的通信消息 $Hello^n$、$A||B^n$、C^n、R_n、$D||E^n$。此时标签和读写器依然能相互认证。

b)在第 *n*+1 次认证的时候，再次阻塞认证协议第⑤步。此时读写器拥有的信息是(TID^{n+2}_{new}，TID^{n}_{old}，K^{n+2}_{inew} (i=1,2)，K^{n}_{iold} (i=1,2)，G_{n+2}，G_{n+3}，r_{n+2}，*ID*)，标签拥有的信息为(TID^{n}_{old}，K^{n}_{iold}(i=1,2)，*ID*，r_{n+2})。

c)重放第一步中听到的消息，首先读写器向标签发送 $Hello^n$，标签返回他的 TID^{n}_{old}，再按照步骤发送 $A||B^n$，然而和之前不同的是，标签的应答消息结合了标签和读写器的新一轮同步化随机数 r_{n+3}，攻击者收到后再重放第一步中的消息 $D||E^n$时，由于 E^n里含有的是前两轮的同步化随机数 r_{n+1}，所以无法通过验证，读写器认证失败，协议终止。从而阻止了去同步化攻击。

7）前向后向安全性

在协议的认证中即使攻击者通过某种方式获取了某一轮的密钥 K_i，G_n，G_{n+1}，但是由于没有时刻跟踪标签，标签和读写器进行了若干次认证，更新了之前的 K_i，G_n，G_{n+1} 等信息。一段时间后，攻击者之前得到的密钥以及认证对将无法再用来进行验证。且在密钥更新过程中，使用 *CRC*、*Cro* 和随机数 N_1、N_2、r_{n+1} 以及 G_{n+1} ,G_{n+2} 计算得到新的密钥，使得攻击者无法从本次获得的密钥推出之后的密钥，保证了协议的前向安全性。

在协议的整个过程中，每轮协议产生的随机数无法预测，保证了各条信息每轮认证都不相同，且攻击者无法从 G_{n+2} 逆推 G_{n+1} 等之前的认证对。因此攻击者无法通过本次攻击的得到的信息，推出之前协议认证的消息内容。故该协议具有后向安全性。

8）双向认证

新协议实现了读写器和标签的相互认证。读写器通过自身产生的随机数 *TID*、N_1、(G_n, G_{n+1})以及密钥 K_i 来认证标签的合法性，标签通过自身 PUF 计算的 G_{n+1}、r_{n+1} 及密钥 K_i 来验证读写器的合法性。满足了双向认证的要求。

表 1 是新协议与 Yang 的协议进行比较。Y 表示能抵抗该种攻击，N 表示不能抵抗该种攻击。如表所示，新的协议比 Yang 的协议具有较高的安全性。

表 1　新协议与其他协议的安全性比较

Table 1　Security comparison between new and other protocols

攻击类型	Yang 的协议	新协议	文献 4	文献 6
假冒攻击	Y	Y	Y	Y
信息泄露攻击	Y	Y	Y	Y
跟踪攻击	N	Y	N	N
克隆攻击	N	Y	N	N
重放攻击	Y	Y	N	Y
去同步化攻击	N	Y	N	N
前向后向安全	Y	Y	Y	Y
双向认证	Y	Y	Y	Y

4　协议的性能分析

本节从标签的计算操作、存储空间、通信成本三方面来讨论新协议的性能。假设协议中所有消息的长度为 L。

计算代价上来说，本文与改进前的协议相比，除了 *CRC*、*Cro* 和⊕操作外，多了一个 PUF 操作，总的来说这四种运算都是一些轻量级运算，计算开销小，很容易在标签中实现。而协议中开销较大的两个随机数的产生放在了读写器，提高了协议的计算效率。

存储量来说，新协议在原协议的基础上由于 PUF 的引入而减少了一个密钥 K_i，但新的协议中标签需要存储一个同步化随机数，所以标签需要存储$\{ID,TID,r_n,K_1,K_2\}$,存储量不变，仍为 5L。

通信成本上来说，新协议在一次完整的认证过程中需要发送一个 TID 以及消息 *R* 和 *C*。总的通信量为 3L。

表 2 是与其他一些算法的比较。

表 2　新协议与其他的协议的性能比较

Table 2　Performance comparison between new and other protocols

协议名	计算代价	存储量	通信成本
文献[4]	∧,∨,⊕,+,Rot,	7L	2L
文献[6]	⊕,+,Rot,MixBit	7L	2L
文献[15]	Rabin,⊕,&	5L+标志位	3L
本文协议	CRC, Cro,⊕,PUF	5L	3L

5　结束语

RFID 技术自出现以来，一直存在许多安全问题。本文对 Yang 的提出的一种轻量级 RFID 的协议的安全性的不足进行了分析，并用物理不可克隆函数（PUF）改进，提出了一种新的协议。经过分析，与原来的协议相比具有更高的安全性，在保证协议效率的同时能抵抗更多的攻击方法、满足更多的安全需求。综上所述，新的协议具有低成本、高效率、高安全性等特点，非常适用于轻量级 RFID 系统。

参考文献：

[1] 周永彬，冯登国. RFID 安全协议的设计与分析 [J]. 计算机学报, 2006, 29 (4): 581-589. (Zhou Yongbin, Feng Dengguo. Design and analysis of cryptographic protocols for RFID [J]. Chinese Journal of Computers, 2006, 29 (4): 581-589.)

[2] Yu Wenjin, Jiang Yixiang. Mobile RFID mutual authentication protocol based on hash function [C]// Proc of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Piscataway,NJ: IEEE Press, 2017: 358-361.

[3] Shi Zhicai, Chen Jiwei, Chen Shanshan, *et al.* A lightweight RFID authentication protocol with confidentiality and anonymity [C]// Proc of the 2nd IEEE Advanced Information Technology, Electronic and Automation Control Conference.Piscataway,NJ: IEEE Press, 2017: 1631-1634.

[4] Chien H Y. SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity [J]. IEEE Trans on Dependable and Secure Computing, 2007, 4 (4): 337-340.

[5] Cao Tianjie, Bertino E, Lei Hong. Security analysis of the SASI protocol [J]. IEEE Trans on Dependable and Secure Computing, 2009, 6 (1): 73-77.

[6] Peris-Lopez P, Hernandez-Castro J C, Tapiador J M. *et al.* Advances in ultralightweight cryptography for low-cost RFID tags: gossamer protocol [C]// Proc of the 9th International Workshop on Information Security Applications. Springer-Verlag, 2009: 56-58.

[7] Bilal Z, Masood A, Kausar F. Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: gossamer protocol [C]// Proc of International Conference on Network-Based Information Systems. Piscataway,NJ: IEEE Press, 2009: 260-267.

[8] Tian Yun, Chen Gongliang, Li Jianhua. A new ultralightweight RFID authentication protocol with permutation [J]. IEEE Communications Letters, 2012, 16 (5): 702-705.

[9] Taqieddin E, Sarangapani J. Vulnerability analysis of two ultra-lightweight RFID authentication protocols: RAPP and gossamer [C]// Proc of the 7th International Conference for Internet Technology and Secured Transactions. Piscataway,NJ: IEEE Press, 2012: 80-86.

[10] 马庆，郭亚军，曾庆江，等. 一种新的超轻量级 RFID 双向认证协议 [J]. 信息网络安全, (Ma Qing, Guo Yajun, Zeng Qingjiang, *et al.* A new ultra-lightweight RFID mutual authentication protocol [J]. Netinfo Security, 2016 (5): 44-50.)

[11] 张兴，李畅，韩冬，等. 基于 Hash 轻量级 RFID 安全认证协议 [J]. 计算机工程与设计, 2018, 39 (5): 1269-1275. (Zhang Xing, Li Chang, Han Dong, *et al.* Lightweight security authentication protocol for RFID based on hash functions [J]. Computer Engineering and Design, 2018, 39 (5): 1269-1275.)

[12] 杨昕，凌捷. 一种低成本超轻量 RFID 双向认证协议 [J]. 计算机科学，2016, 43 (4): 160-162. (Yang Xin, Ling Jie. Low-cost

ultralightweight RFID mutual-authentication protocol [J]. Computer Science, 2016, 43 (4): 160-162.)

[13] 柳毅, 顾国生. 一种新的轻量级 RFID 双向认证协议 [J]. 计算机科学, 2017, 44 (2): 206-208. (Liu Yi, GuGuosheng. New mutual authentication for lightweight RFID protocols [J]. Computer Science, 2017, 44 (2): 206-208.)

[14] 马远佳, 刘道微. 一种改进的满足后向安全的 RFID 双向认证协议 [J]. 计算机工程与应用, 2017, 53 (9): 136-140. (Ma Yuanjia, Liu Daowei. Improved mutual authentication with backward security for RFID protocols. Computer Engineering and Applications, 2017, 53 (9): 136-140.)

[15] 魏棉裕, 欧毓毅. 改进的抗去同步化攻击 RFID 安全协议 [J]. 计算机工程与设计, 2017, 38 (7): 1719-1723. (Wei Mianyu, Ou Yuyi, Improved resistance de-synchronization attack RFID security protocol [J]. Computer Engineering and Design, 2017, 38 (7): 1719-1723.)